**IN THE CLAIMS:**

1.      **(Previously Presented)** A PKI certificate architecture for a network connected gaming system, the gaming system including a plurality of gaming machines each having a plurality of executable software components, wherein each different executable software component within each gaming machine within the gaming system subject to receive certification is uniquely associated with a unique identifier and is signed with a separate and unique PKI certificate, the separate and unique PKI certificate being uniquely identified at least by the unique identifier, wherein identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are signed with identical PKI certificates, such that non-identical executable software components in different ones of the plurality of gaming machines are associated with separate and different identifiers and are signed with separate and different PKI certificates, and such that no two non-identical executable software components in different gaming machines are signed with a same PKI certificate.

2.      **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein each software component is authorized by a regulatory authority.

3.      **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein the separate and unique PKI certificate is produced by the certification lab, by the gaming system supplier or by the trusted party designated by the regulatory authority.

4.      **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein each software component is code signed by a certification lab, by a gaming system supplier or by a trusted party designated by the regulatory authority.

5.　　**(Previously Presented)** A PKI certificate architecture according to claim 1, wherein the separate and unique identifier is a certificate field selected from a "Subject" field, an "issued to" field, a "subject name" field, a "CommonName" field, a "provider" field or a "publisher" field.

6.　　**(Previously Presented)** A PKI certificate architecture according to claim 1, wherein the unique identifier comprises at least one of fields and field extensions.

7.　　**(Previously Presented)** A PKI certificate architecture according to claim 1, wherein the unique identifier comprises at least one of a plurality of fields selected from among:

a software component part number;

a software component major version number;

a software component minor version number;

a software component build number;

a software component revision number;

a software component project name;

a software component type of software component;

a software component language variant;

a software component game regulation variant;

a software component friendly name;

an identification of the certification laboratory, and

an identification of the client.

8.　　**(Previously Presented)** A PKI certificate architecture according to claim 7, wherein the unique identifier is a concatenation of selected identifiers.

9. **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is reported in the Windows event log upon execution of the software component.

10. **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is reported in the source field of the Windows event log upon execution of the software component.

11. **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is reported in the Windows event log upon execution of the software component in a predetermined event log bin upon execution of the software component.

12. **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein at least a portion of the unique identifier is traceable in at least one of:

source code;

Windows File Properties;

Trusted Inventory;

Windows Event Log;

Software Restriction Policies, and

Certificate Store.

13. **(Original)** A PKI certificate architecture according to claim 1, wherein the network connected gaming system is connected in at least one of a local area system and wide area network.

14.    **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein the network connected gaming system comprises at least one of gaming terminals, gaming servers and computers.

15.    **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein the unique identifier contains identification information delimited with file-name-allowed non-alphanumeric characters to facilitate human identification, string searches and file searches.

16.    **(Previously Presented)** A PKI certificate architecture according to claim 1, wherein a selected set of identification information making up the unique identifier are used for making up the file name of PKI certificate related files such as *.CER, *.P7B and *.PVK such as to facilitate human identification, string searches and file searches.

17.    **(Previously Presented)** A method for a network connected gaming system to prevent unauthorized software components of constituent computers of the gaming system from executing, the gaming system including a plurality of gaming machines each having a plurality of executable software components, the method comprising the steps of:

producing a separate and unique PKI certificate for each of the plurality of executable software component subject to receiving certification within each gaming machine, each software component subject to receiving certification including a unique identifier;

code signing each executable software component subject to receiving certification with its respective separate and unique PKI certificate, each respective PKI certificate being uniquely identified at least by a unique identifier that is uniquely associated with the executable software component such that identical executable software components in different ones of the plurality

of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates, such that non-identical executable software components in different ones of the plurality of gaming machines are associated with separate and different identifiers and are code signed with separate and different PKI certificates and such that no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate, and

configuring software restriction policy certificate rules to allow execution of only those executable software components whose code signed PKI certificate is determined to be authorized.

18.    **(Previously Presented)** A method according to claim 17, further comprising the step of configuring software restriction policy rules to prevent execution of unauthorized software components.

19.    **(Previously Presented)** A method according to claim 17, further comprising the step of configuring software restriction policy rules to prevent execution of all not explicitly authorized software components.

20.    **(Previously Presented)** A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute, comprising the steps of:

code signing each authorized software component with a PKI certificate such that identical authorized software components in different ones of the constituent computers are code signed with identical PKI certificates, such that non-identical authorized software components in different ones of the constituent computers are code signed with separate and different PKI

certificates and such that no two non-identical authorized software components in different ones of the constituent gaming machines are code signed with a same PKI certificate;

configuring a separate software restriction policy for each authorized software component in each of the constituent computers of the gaming system, and associating the configured separate software restriction policy with the PKI certificate with which the authorized software component was code signed;

enforcing the associated software restriction policy for each code signed authorized software component such that each code signed authorized software component in each of the constituent computers of the gaming system must be authorized to run by its associated separate software restriction policy.

21.     **(Previously Presented)** A method according to claim 20, wherein the authorized software components are mandated by a regulatory body.

22.     **(Previously Presented)** A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute, comprising the steps of:

configuring a separate and unique certificate software restriction policy for each authorized executable software component of each of the constituent computers of the gaming system such that the each authorized executable software component in each of the constituent computers of the gaming system must be authorized to run by its associated separate software restriction policy;

code signing each authorized software component with a PKI certificate such that identical authorized software components in different ones of the constituent computers are code

signed with identical PKI certificates, such that non-identical authorized software components in different ones of the constituent computers are code signed with separate and different PKI certificates and such that no two non-identical authorized software components in different ones of the constituent gaming machines are code signed with a same PKI certificate;

configuring a path software restriction policy to prevent unauthorized software components from executing;

configuring a path software restriction policy to prevent non-explicitly authorized software components from executing;

enforcing the certificate software restriction policy configured for each of the code signed authorized executable software components of each of the constituent computers of the gaming system, and

enforcing the path software restriction policies.

23.    **(Previously Presented)** A method according to claim 22, wherein the authorized software components are mandated by a regulatory body.

24.    **(Previously Presented)** A method for a network connected gaming system to enable only authorized software components of constituent computers of the gaming system to execute, the gaming system including a plurality of gaming machines each having a plurality of executable software components, the method comprising the steps of:

producing a separate and unique PKI certificate for each of the plurality of executable software components within the gaming system subject to receive certification, each respective PKI certificate being associated with a unique identifier that is uniquely associated with the executable software component such that identical executable software components in different

ones of the plurality of gaming machines of the network connected gaming system are associated with identical identifiers and are code signed with identical PKI certificates, such that non-identical executable software components in different ones of the plurality of gaming machines are code signed with separate and different PKI certificates and such that no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate;

code signing each software component subject to receive certification with its respective separate and unique PKI certificate;

configuring a certificate software restriction policy for each of the respective separate and unique PKI certificates, and

enforcing the certificate software restriction policy for each of the respective separate and unique PKI certificates.

25.    **(Previously Presented)** A method for downloading authorized executable software components and allowing execution of downloaded authorized executable software components of a plurality of gaming machines of a network connected gaming system, comprising the steps of:

for each of the plurality of gaming machines of the network connected gaming system:

code signing each authorized executable software component with a separate PKI certificate that is unique to the authorized software component such that identical executable software components in different ones of the plurality of gaming machines of the network connected gaming system are code signed with identical PKI certificates, such that non-identical authorized software components in different ones of the plurality of gaming machines are code

signed with separate and different PKI certificates and such that no two non-identical authorized software components in different gaming machines are code signed with a same PKI certificate;

packaging the code signed authorized software components into an installation package;

configuring install policies to install each code signed authorized executable software component contained in the installation package;

configuring certificate rule policies to allow execution of the installed code signed authorized executable software component;

configuring enforcement of the policies.

26-81. **(Canceled)**

82. **(Previously Presented)** An automated platform to enable an on-going regulatory certification of a plurality of authorized software components of a network connected gaming system including a plurality of computers, the method comprising:

a reference platform representative of a target network connected gaming system and comprising a software-building environment located at a manufacturer or subcontractor of the software components;

a certification platform located at a regulatory certification authority, the certification platform being substantially identical to the reference platform, and

code-signing means for enabling the manufacturer or subcontractor to associate a separate and unique PKI certificate with each authorized software component subject to regulatory certification such that identical authorized software components subject to regulatory certification in different ones of the plurality of gaming machines of the network connected

gaming system are code signed with identical PKI certificates, such that non-identical executable software components in different ones of the plurality of gaming machines are code signed with separate and different PKI certificates, and such that no two non-identical executable software components in different gaming machines are code signed with a same PKI certificate.

83.    **(Previously Presented)** An automated platform according to claim 82, further comprising a secure communication link between the reference platform and the certification platform for enabling manufacturer or designated subcontractors to remotely configure the software building environment on the certification platform.

84.    **(Previously Presented)** An automated platform according to claim 82, wherein the authorized software components to be downloaded to the network connected gaming system are tested by the certification laboratory.

85.    **(Previously Presented)** An automated platform according to claim 82, wherein the authorized software components to be downloaded to the network connected gaming system are compiled by the certification laboratory.

86.    **(Previously Presented)** An automated platform according to claim 82, further comprising a secure communication link between the reference platform and the certification_for enabling remote assistance.

87.    **(Previously Presented)** An automated platform according to claim 82, further comprising a secure communication link between the reference platform and the certification_for enabling users to carry out certification steps from a remotely located computer.

88. **(Original)** An automated platform according to claim 82, wherein the code signing means comprises a certificate authority under control of the manufacturer for generating certificates.

89. **(Original)** An automated platform according to claim 82, wherein the code signing means comprises a certificate authority under control of the regulatory certification authority for generating certificates.

90. **(Previously Presented)** An automated platform according to claim 82, further comprising means for maintaining the software-building environment of the reference platform and the software-building environment of the certification platform synchronized.

91-97. **(Canceled)**